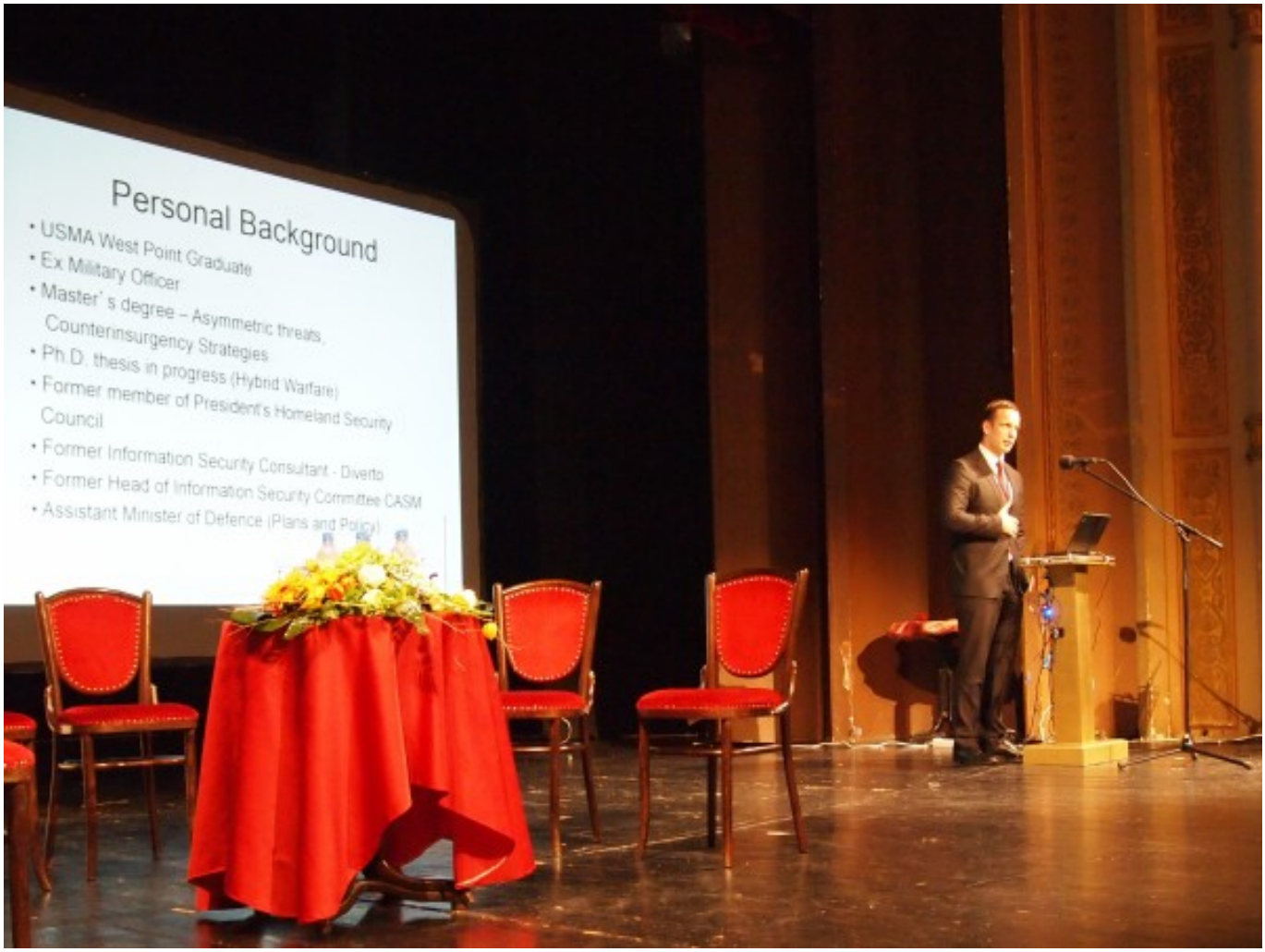
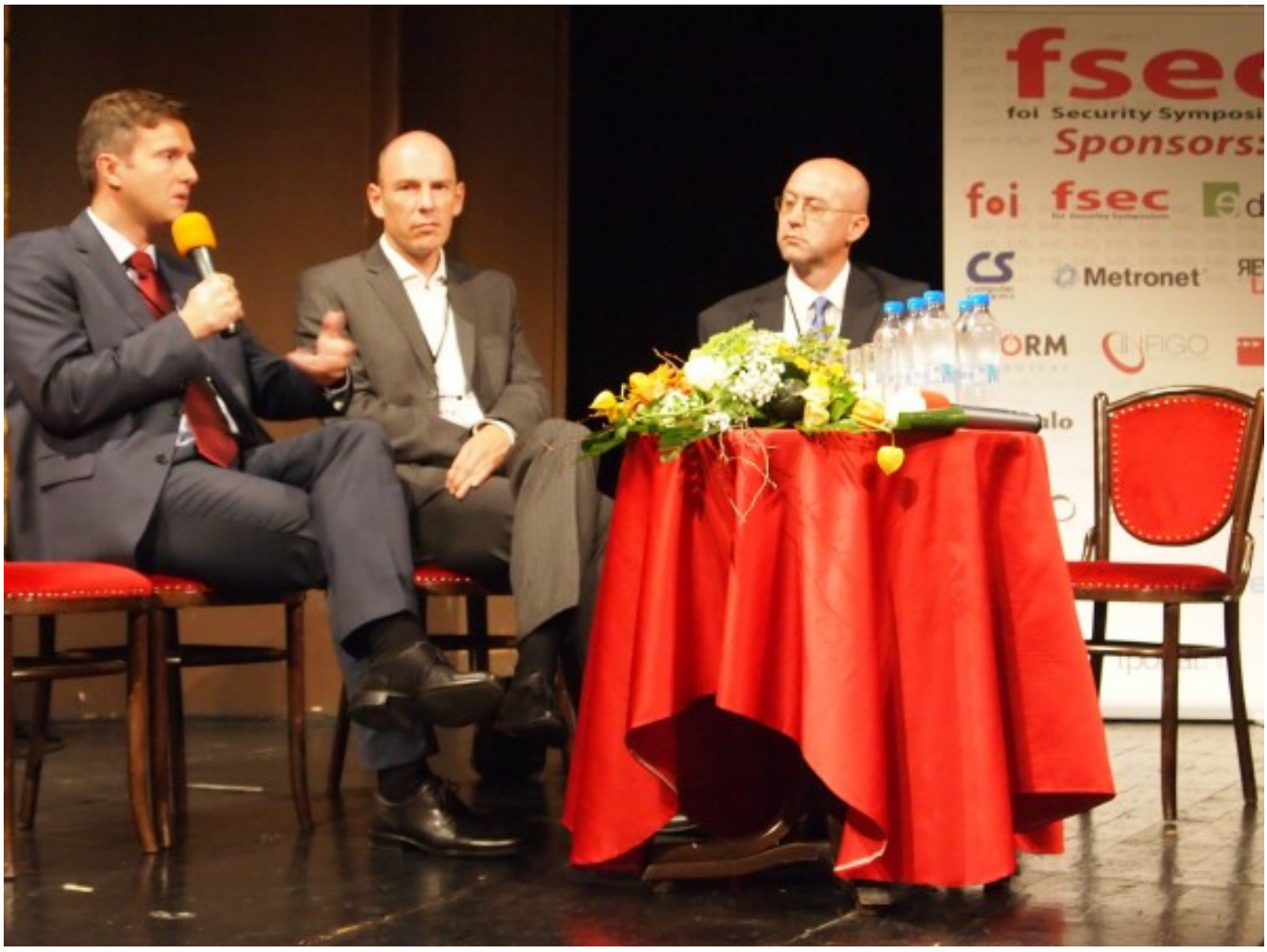
Konferencija FSEC 2016

Ovogodišnji FSEC [1] promijenio je mjesto održavanja: umjesto na FOI-u, održan je u varaždinskom Hrvatskom narodnom kazalištu, koje iznutra izgleda kao umanjeno izdanje zagrebačkog HNK. Iako je i FOI smješten u starom zdanju, nekadašnjem samostanu, ipak je sudionicma trebalo par trenutaka da se prilagode okruženju. Nove tehnologije predstavljene u starom zdanju - zanimljiv kontrast koji bi se mogao shvatiti kao metafora za cijelo naše društvo, koje je još zarobljeno prošlošću, a krajnje je vrijeme da se okrene budućnosti. Predavači su se obraćali publici s "dasaka koje život znače".



FSEC je moja omiljena konferencija. Zamišljena kao "vendor neutralna", od prvih je dana bila okupljalište zaigranih hakera koji su publici, uglavnom sastavljenoj od istih takvih hakera, uz primjesu sudionika iz akademske zajednice i ponekog sigurnjaka iz državnog sektora, prezentirala svoje omiljene igračke. No treba pokriti troškove, pa su tu uvijek bili prisutne i sponzorske tvrtke, ali na diskretan način. Informacijska sigurnost je široko područje, koje se može sagledavati s raznih strana, i upravo je u tome trajna vrijednost ove konferencije, koja pruža mogućnost učenja i širenja horizonata.

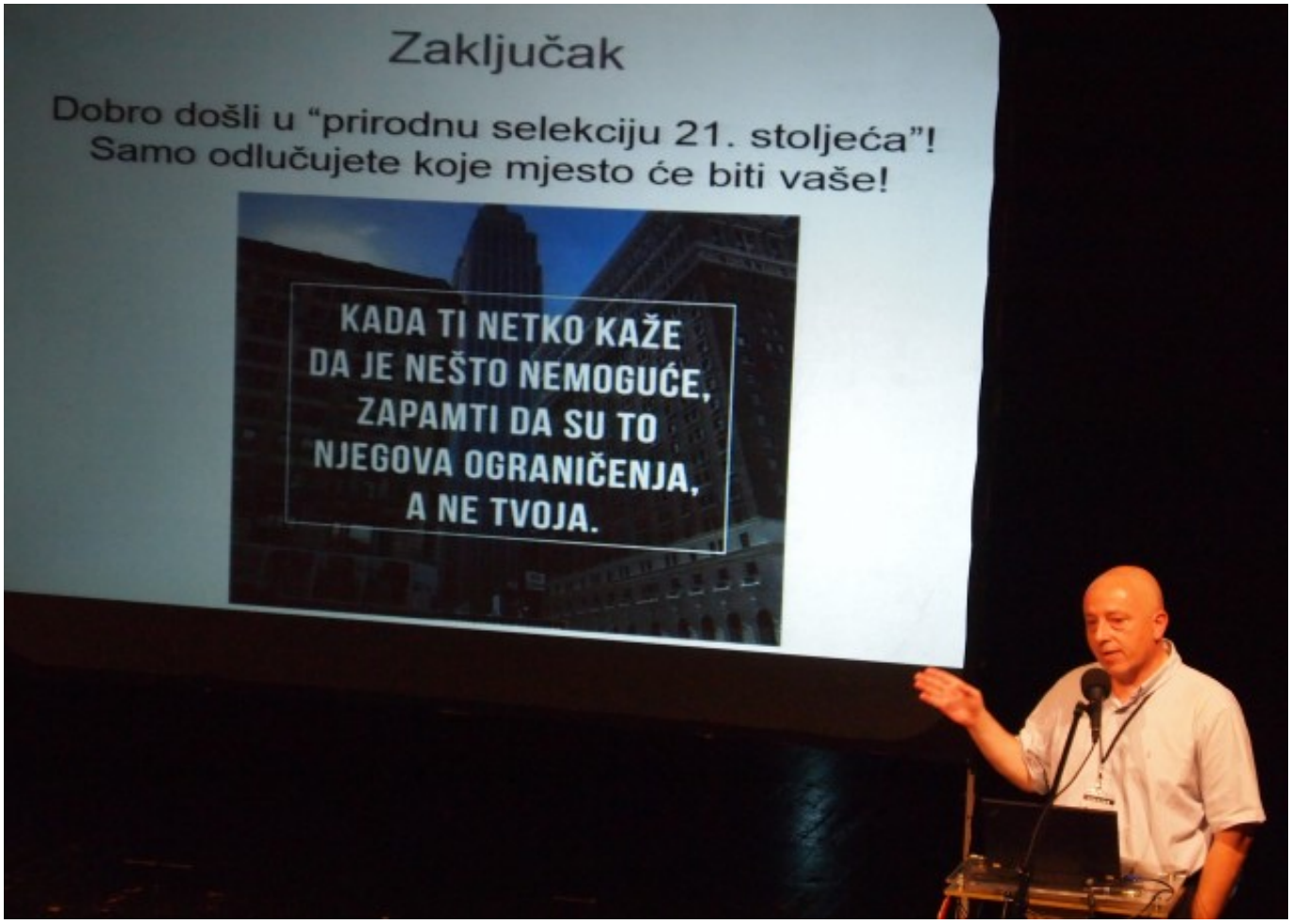
Kako prolaze godine, tako se širi lista sudionika i predavača. Ove su godine prva predavanja odradili predavači iz državnog i privatnog sektora. Uvodno predavanje održao je Nikola Brzica iz Ministarstva obrane. Prenio nam je kako NATO i Hrvatska kao njegova članica gledaju na *cyber warfare*. Podsjetio nas je na Clausewitzovu definiciju rata kao kontroliranog sukoba koji nastaje kao nastavak politike radi ostvarivanja konkretnih ciljeva, ali i na Sun Tzuovu tvrdnju da je naviše umijeće ratovanja kad postigneš pobjedu bez borbe. Drugi svjetski rat pokazao je svima kamo vodi rat kao golemo, bezumno razaranje i isrpljivanje, dakle nešto posve suprotno Sun Tzuovoj filozofiji. Danas se ratovi vode "pametnije", sve su više asimetrični, grupe država/savezi ratuju protiv jedne države ili jedne političke grupacije. Nakon cyber napada na Estoniju, kada su NATO-ovi informatičari morali priskočiti u pomoć, NATO je proširio definiciju ratovanja, ustvrdivši da *cyber war* može izazvati velika razaranja i štete jednako kao i klasični rat. Zapravo se više koristi termin *cyber warfare*, koji označava tihi rat, koji nije objavljen, ali se događa svakodnevno. Radi se o prikupljanju informacija o potencijalnim protivnicima, traženju njihovih slabosti, uključujući i slabosti informacijskih sustava. Time je zahvaćen i privatni sektor, koji mora čuvati svoje poslovne tajne od konkurencije. Brzica u svom izlaganju nije ni spomenuo obične građane i njihov položaj u svijetu stalno tinjajućeg sukoba velikih igrača. No ruku na srce, NATO se i ne bavi zaštitom privatnosti građana, a ta je tema obrađena u popodnevnom turnusu.



Uslijedio je okrugli stol koji se bavio raspravom o kritičnoj nacionalnoj infraskturi. Sudjelovali su predstavnici dva telekoma (Metronet i VIP) i Zagrebačke banke, i profesionalci iz državnog sektora, iz UVNS-a i ZSIS-a. Čini se da je tema kritične infrastukture nekako nametnuta priključivanjem EU i NATO savezu, pa se naša država još prilagođava - takav se utisak stiče iz nekoliko primjera koje smo čuli. Naime radi se o listi organizacija koje pružaju usluge koje su neophodne za funkcioniranje društva, a mogu biti ugrožene u slučaju prirodnih nepogoda ili rata. Telekomi spadaju u kritičnu infrastrukturu, a i dio bankarskih usluga, istaknuli su sugovornici iz privatnog sektora. Oni uglavnom sami financiraju ulaganja u svoju infraskturu, na što ih prisiljava konkurencije i želja da zadrže

klijente, ali i regulativa. Narodna banka je tu odradila dobar posao, postavivši bankama visoke standarde. Tamo gdje još postoje monopoli država bi trebala odigrati svoju ulogu. Briga o kritičnoj infrastukturi važan je dio upravljanja svakom razvijenom i civiliziranom državom.

Ivica Ostojić iz tvrtke Diverto bavio se temom Fintecha, odnosno promjenama koje Internet i IT tehnologije donose financijskom sektoru. Po njemu će kriptovalute i *blockchain* tehnologija izazvati ogromne promjene u svijetu. *Coini* više nisu samo *geek* tehnologija, a *blockchain* se može primijeniti na brojne oblasti, poput zemljišnih knjiga, ugovora, knjigovodstva itd. Promjene koje nas čekaju dovest će do izumiranja pojedinih zanimanja: spomenuo je bilježnike, jer više neće trebati ovjeravati ugovore i potpise, računovođe, a i banke koje se na vrijeme ne prilagode bit će osuđene na propast. Konzorciji banaka u tišini razvijaju svoje verzije Bitcoina, jer su već prevazišli faze negiranja i ljutnje, sada su, po Ostojiću, u fazi "pregovaranja", odnosno nastoje iz blockchaina izvući samo ono što im odgovara. Teško mogu progutati decentraliziranost čuvanja "glavne knjige" (general ledger), jer su navikli čuvati podatke kod sebe. Takav pristup osuđen na propast, jer bi se time uzgrozila osnovna ideja, transparentnost i neporecivost svih transakcija, pa će biti prisiljeni prihvatiti tehnologiju onako kako je i zamišljena. Veliki igrači se pripremaju zauzeti pozicije i osigurati sebi lavovski dio kolača, dok se javnost smišljeno drži u neznanju. O Bitconu se u medijima govori uglavnom u negativnom kontekstu, radi (pseudo) anonimnosti koja omogućava prikrivanje transakcija. Međutim mnoge kriptovalute koji nastaju nakon Bitcona omogućavaju posvemašnju transparentnost, svaka transakcija nosi ID pravne ili fizičke osobe, tako da će država moći pratiti protok novca. S druge strane, nastaju nove valute koje omogućuju još veću anonimnost nego Bitcoin. Vrijeme će pokazati koje će od tih valuta preživjeti, ojačati, a koje će nestati u zaboravu. U svakom slučaju, svatko tko je dalekovidan sada ima priliku priskrbiti sebi dio buduće zarade i osigurati si blagostanje.



Pravnoj zaštiti naše privatnosti bilo je posvećeno predavanje Gorana Vojkovića. Postojeća je regulativa manjkava, onemogućuje pravnu zaštitu izvan državnih granica. Kako možemo biti sigurni tko pristupa našim podacima koji su smješteni negdje u oblaku, smještenom na drugom kontinetu, na primjer ako koristimo, kao dobar dio Akademske zajednice, Office 365?

Kako se hakeri nose s obradom velikih količina podatka pokazao je Milan Gabor u prezentaciji When hacker meets big data. Uz pomoć pravih alata mogu se izvlačiti uzorci i izraditi zanimljive vizualizacije.

Sladokusce će zaintrigirati minijaturno računalo smješteno na USB sticku, tvrtke Inverse Path. To je open source projekt koji će zagolicati maštu svakog *geeka*: Više na ovom linku [2].

Nadam se da će ovih nekoliko odlomaka biti dovoljno da prenese duh ove konferencije. Osim spomenutih, FSEC je ponudio još mnoštvo zanimljivih predavanja, tako da smo otišli kući s novim znanjima i s još više otvorenih pitanja o kojima tek treba razmisliti. U tome je i najveća vrijednost ove konferencije: tjera nas na razmišljanje. Ako ste je propustili ove godine, toplo vam preporučujem da je ne propustite nagodinu.

Raspored predavanja dostupan je ovdje [3], a uskoro će na stranicama konferencije biti objavljena i većina prezentacija.

sub, 2016-09-17 17:21 - Aco Dmitrović**Vijesti:** Događanja [4]
Kategorije: Sigurnost [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1677

Links
[1] http://fsec.foi.hr/
[2] https://frab.fsec.foi.hr/en/FSec2016/public/events/11
[3] https://frab.fsec.foi.hr/en/FSec2016/public/schedule
[4] https://sysportal.carnet.hr./taxonomy/term/43
[5] https://sysportal.carnet.hr./taxonomy/term/30